数理解析研究所講究録 1451 巻 2005 年 61-71

p-adic Diophantine Approximations on Tate curves and the abc-conjecture

Noriko HIRATA-KOHNO

December, 2004

Abstract

In this article, we present Diophantine Approximations on Tate elliptic curves, so-called linear forms in p-adic elliptic logarithms. We give fundamental known concepts on Tate elliptic curves and arithmetical properties.

We also describe how are deduced applications around the abc-conjecture from the theory of p-adic linear forms in usual logarithms.

Keywords: linear forms in p-adic logarithms, Tate curves, elliptic curves, elliptic logarithms, the abc-conjecture.

1 Introduction

pを素数とする．ここではTate curveと呼ばれる楕円曲線における，p進ディオファントス近似と，Lutz-Weilのp進楕円対数のディオファントス近似について考察する．

p進付値におけるp進楕円対数の近似は，通常のアルキメデス付値でのそれとほぼ同様の現象を示すが，これはabc予想，そしてabc予想に深く関連する楕円曲線におけるSzpiro予想，及び，楕円曲線周期予想に向かうための重要な布石である．

abc予想とは「整数は，アルキメデス付値と素数pでの振る舞いの関係が極めて理想的にコントロールされている状況しか許さない」と言う予想なのであるから．

このテキストにおける結果では，abc 予想に対する直接の肯定も否定も全く出来ない．

しかし，楕円対数の p 進ディオファントス近似ではなく，通常の対数の p 進ディオファントス近似が「abc 予想の exponential 分だけ大きすぎる評価」を導くことを簡単に説明する．

そして楕円対数のディオファントス近似を用いると，通常の対数ディオファントス近似の直接の応用の場合に比べて「log 分だけ小さい評価」に至る評価改良が，可能になる例のあることのみ，言及しておこう．

2 Preliminaries

K を有理数体 $\mathbb{Q}$ 上有限次元 D の代数体とする．$|\cdot|$ を K の通常のアルキメデス付値，p を $\mathbb{Q}$ の素数とする．p の上の K の素点の一つ v をとる．ここで考える p 進付値 $|\cdot|_v$ は $x \in \mathbb{Q}$ に対して $|x|_v = p^{-ord_p(x)}$ を満たすように正規化されているとする．K_v を K の v による完備化とし，$\mathbb{Q}_p$ を $\mathbb{Q}$ の p による完備化とする．

体 K_v は $\mathbb{Q}_p$ の有限次拡大体となる．その拡大次数を local degree と呼び $d_v = [K_v : \mathbb{Q}_p]$ とおく．$\mathbb{C}_p$ を K_v の代数閉包の完備化とする（K_v の代数閉包は一般に完備ではない）．$\mathbb{C}_p$ は標数 0 の完備な代数閉体となり，そこで K_v の代数閉包は dense となる．

q を $0 < |q|_v < 1$ を満たす K_v の元とする．Eisenstein 級数 E_4 及び E_6 を次のように定める：

$$E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n} \tag{1}$$

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n} \tag{2}$$

さらに Jacobi-Tate の楕円関数 $\wp_q$ を次のように定義する：

$$\wp_q(z) = \sum_{n \in \mathbb{Z}} \frac{q^n z}{(1 - q^n z)^2} + \frac{1}{12} - 2 \sum_{n=1}^{\infty} \frac{n q^n}{1 - q^n} \tag{3}$$

$\wp_q(z)$ は $K_v - \{0\}$ で meromorphic であり，乗法的周期 q をもつ周期関数である．微分作用素 $D := z\frac{d}{dz}$ を考えると

$$D\wp_q(z) = \sum_{n\in\mathbb{Z}} \frac{q^n z + q^{2n}z^2}{(1-q^n z)^3} \tag{4}$$

であり，これらの関係は通常の場合と同様に

$$\mathcal{E}(q)\ :\ D\wp_q(z)^2 = 4\wp_q(z)^3 - \frac{1}{12}E_4(q)\wp_q(z) + \frac{1}{216}E_6(q) \tag{5}$$

となる [Ro]．これから作られる写像

$$z \mapsto (\wp_q(z), D\wp_q(z)) \tag{6}$$

は $K_v^* := K_v - \{0\}$ から K_v^2 への写像であり，Lie 群の解析的準同型写像となって $K_v^*/q^{\mathbb{Z}}$ と $\mathcal{E}(q)$ の間の同型を与える．またテータ級数（通常のテータ級数と $\prod_{n=1}^{\infty} \frac{1}{(1-q^n z)^2}$ だけ異なる，[Ro] 参照）は

$$\Theta_q(z) := (1-z^{-1}) \prod_{n=1}^{\infty} \frac{(1-q^n z^{-1})(1-q^n z)}{(1-q^n z)^2} \tag{7}$$

で与えられ，(7) のテータ級数を乗ずることで (3) の極を射影空間において「消去」して (6) から得られる正則な同型写像の射影座標表示は

$$z \mapsto (\Theta_q(z)^3, \Theta_q(z)^3\wp_q(z), \Theta_q(z)^3 D\wp_q(z)) \tag{8}$$

である．

これらは全て Tate 以来よく知られている事実である．また $R \neq 0$，$f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$ に対して $|f(z)|_R := \max\{|a_n R^n|_v; n \in \mathbb{Z}\}$ とおくと具体的なこれらの関数の挙動として

$$|\Theta_q(z)^3|_R \le \exp\left(\frac{3(\log R)^2}{-2\log|q|_v} + \frac{3|\log R|}{-2\log|q|_v} - \frac{3\log|q|_v}{8}\right)$$

$$|\Theta_q(z)^3\wp(z)|_R \le |\frac{1}{12}|_v \exp\left(\frac{3(\log R)^2}{-2\log|q|_v} + \frac{3|\log R|}{-2\log|q|_v} - \frac{3\log|q|_v}{8}\right)$$

$$|\Theta_q(z)^3 D\wp(z)|_R \le \exp\left(\frac{3(\log R)^2}{-2\log|q|_v} + \frac{3|\log R|}{-2\log|q|_v} - \frac{3\log|q|_v}{8}\right)$$

および $|z|_v = R$ を満たす全ての $z \in K_v^*$ に対して次が得られる（[Ro],[Da]）:

$$\max\left\{|\Theta_q(z)^3|_R\ |\Theta_q(z)^3 D\wp(z)|_R\right\} \ge \exp\left(\frac{3(\log R)^2}{-2\log|q|_v} + \frac{3|\log R|}{-2\log|q|_v}\right).$$

注意するべき事は，最初から (5) の式が K 係数であるように与えたのではないと言うことである．p 進ではない複素数の場合，楕円曲線 E を $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\tau \in \mathcal{H}$ に対するトーラス $\mathbb{C}/\Lambda$ と見なすと $\{q^{\mathbb{Z}}\} = \exp(2\pi i\Lambda)$ なる $q = \exp(2\pi i\tau)$ に対して $\mathbb{C}^*/q^{\mathbb{Z}}$ が $E(\mathbb{C})$ と同型になるのであり，その定義式は $\mathbb{Z}[[q]]$ 係数である．

このような通常の複素数の場合，invariants g_2, g_3 が代数的数，という仮定の下で $\wp$ の零でない周期は超越的で，かつ π とは $\overline{\mathbb{Q}}$ 上一次独立であり，このことから $0 < |q| < 1$ となる複素数 $q = \exp(2\pi i\tau), \tau \in \mathcal{H}$ に対しては $E_4(q)$ と $E_6(q)$ の少なくとも一方は超越数と言う結果が出る事に注意しよう（[Wal] の p.65　系 3.2.9 または [Be]）．E の定義式として Weierstrass の標準形をまず考えるのではなく，Eisenstein series

$$G_{2k}(\tau) := \sum_{m,n\in\mathbb{Z},(m,n)\neq(0,0)} (m+n\tau)^{-2k}$$

に対して $g_2 = \dfrac{60G_4}{\omega_1^4}$, $g_3 = \dfrac{140G_6}{\omega_1^6}$ （$\wp$ の周期を $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ とする）を代数的と仮定するのである．つまり代数的数 g_2, g_3 を超越数 ω_1 で割り算することを考えている事になる．この場合 G_4, G_6 が超越数になるのは当然であるし，上記の「$E_4(q)$ と $E_6(q)$ の少なくとも一方は超越数」と言う結果も

$$G_{2k}(q) := (2\pi i)^{-2k} \sum_{m,n\in\mathbb{Z},(m,n)\neq(0,0)} \left(m\frac{\log|q|}{2\pi i} + n\right)^{-2k}$$

に対して

$$G_{2k}(q) = (2\pi i)^{-2k} \cdot 2\zeta(2k)E_{2k}(q) = (-1)^k \frac{B_k}{(2k)!} E_{2k}(q)$$

に注意しながらアナロジーをなぞっているのだから，さほど驚くような事ではない（ここで B_k はベルヌーイ数なので有理数）．

つまり，楕円曲線の与え方を間違ってはいけない訳である．ここで再び p 進の話に戻る．まず Tate (elliptic) curve とは $q \in \mathbb{C}_p^*, |q|_v < 1$ に対して $\mathbb{C}_p^*/q^{\mathbb{Z}}$ で与えられるものと定義する．この Tate curve $\mathbb{T}$ は $\mathbb{C}_p$ 上定義された種数 1 の非特異な曲線と同型であり，そのような $\mathbb{T}$ はさきの (3) の $\wp_p$ で parametrize されるので (5) の式で与えられる．すなわち Tate curve は

$$Y^2 = 4X^3 - \frac{1}{12}E_4(q)X + \frac{1}{216}E_6(q) \tag{9}$$

で定まる．

さて，最初に楕円曲線 E が代数体 K 上の曲線として与えられたとする．v を代数体 K の素点で，E が bad reduction を持つとすると $E(K_v)$ が $K_v^*/q_v^{\mathbb{Z}}$ と同型になるような $q_v \in K_v$ が存在する．すなわち $E(K_v)$ と，先の $\mathcal{E}(q_v)$ は同型になる．

(5) の式で定められる $\mathbb{T}$ は complex multiplication を持たない事に注意しておこう．

3 Result on Tate curves

p 進の場合の Eisenstein 級数の超越性の結果とその定量版を述べる．

Theorem 1 K を有理数体 $\mathbb{Q}$ 上有限次元 D の代数体とする．β_1, β_2 を K の元とする．$h(\cdot)$ を絶対 logarithmic projective height とする．B を $\log B = \max\{h(\beta_1), h(\beta_2), 1\}$ をみたす実数とする．p を $\mathbb{Q}$ の素数とする．p の上の K の素点の一つ v に対し K_v を K の v による完備化とし，$\mathbb{Q}_p$ を $\mathbb{Q}$ の p による完備化とする．q を $0 < |q|_v < 1$ を満たす K_v の元とする．Eisenstein 級数 E_4 及び E_6 を先のようにとる．このとき，B によらない effective な正定数 $C > 0$ が存在して次を満たす．

$$\max\{|E_4(q) - \beta_1|_v, |E_6(q) - \beta_2|_v\} \geq \exp\{-C(\log B)^2\}$$

Corollary 1 定理 1 と同じく q を $0 < |q|_v < 1$ を満たす K_v の元とする．このとき Eisenstein 級数の値 $E_4(q), E_6(q)$ は，決して同時に代数的数にはならない．

すなわち，Eisenstein series の値については「p 進の場合」についても複素数のときのアナロジーとなる超越性が成立する [Be]．

ここで，「q は代数的数」というたぐいの仮定は一切無く，単に $0 < |q|_v < 1$ を満たす K_v の元としていることにも注意．この点は複素数のときと多少違う．

4 Lutz-Weil の p 進楕円関数の場合

K を再び代数体とする．今度は $\mathcal{E}$ を K 上定義された楕円曲線で $y^2 = x^3 - ax - b$ $(a, b \in O_K)$，$4a^3 \neq 27b^2$ によって定まっているとする．$\lambda_p = \frac{1}{p-1} (p \neq 2$, $\lambda_2 = 3$ とおく．$\mathcal{C}_p := \{z \in \mathbb{C}_p : |z|_v < p^{-\lambda_p}\}$ とし，$\mathcal{C}_v := \mathcal{C}_p \cap K_v$ とおく．$\beta_1, \cdots, \beta_k \in K$ を $|\beta_i|_v \leq 1$ となるように取る．

Lutz-Weil の p 進楕円関数とは次を満たすものである．

$\varphi : \mathcal{C}_v \to K_v$ なる関数で $\varphi(0) = 0$, $\varphi'(0) = 1$ および微分方程式 $(Y')^2 = 1 - aY^4 - bY^6$ を満たすものが存在する事が知られている．

この φ の定義域を $\mathcal{C}_p$ に拡張すると p 進 Lie 群 $\mathcal{E}(\mathbb{C}_p)$ に対して指数写像 $\mathcal{C}_p \to \mathcal{E}(\mathbb{C}_p)$ が次のように定義される：

$$\exp_p(z) = \big(\varphi(z), \varphi'(z), \varphi^3(z)\big)$$

これを Lutz-Weil p 進楕円関数（写像）と呼ぶ．

つまり楕円曲線は $Y^2Z = X^3 - aXZ^2 - bZ^3$ とかけるが，それは $(X, Y, Z) = (\varphi, \varphi', \varphi^3)$ という parametrization に基づく．この φ は locally analytic であり，$\mathcal{C}_p$ 上では解析的だが $\mathbb{C}_p$ では解析的でない．実際 φ は単射奇関数であり，$|\varphi(z)|_v = |z|_v, |\varphi'(z)|_v = 1$ が $z \in \mathcal{C}_p$ の全てに対して成立する．すなわち $\exp_p$ には周期が無い．同じ p 進でも，Jacobi-Tate の方には周期が（たった1つであるが）ある．

Lutz-Weil p 進写像 $\exp_p$ は加法公式，微分公式が通常の Weierstraß 楕円関数と同様に存在する．

この Lutz-Weil p 進の指数写像の逆関数の値にあたる楕円対数についての近似を述べる：

Theorem 2 $\mathcal{E}_1 \cdots, \mathcal{E}_k$ を上記のように $y^2 = x^3 - a_i x - b_i$ $(a_i, b_i \in O_K, 1 \leq i \leq k)$ で定まる楕円曲線とする．$h = \max_{1 \leq i \leq k}\{h(1, a_i, b_i), 1\}$ とおき，楕円対数を各 $1 \leq i \leq k$ に対して

$$0 \neq u_i \in \{u \in \mathcal{C}_v : \exp_p(u) \in \mathcal{E}_i(K)\}$$

と定める．U_i と V_i を $U_i = \dfrac{p^{-\lambda_p}}{|u_i|_v} \quad (>1)$ および

$$\log V_i \geq \max\{h(\exp_p(u_i)),\ \frac{1}{D}\}$$

を満たすような実数とする $(1 \leq i \leq k)$．ただし $U_1 = \max(U_i)$, $V_1 = \max(V_i)$ としておく．さて $\beta_1, \cdots, \beta_k \in K - \{0\}$, $|\beta_i|_v \leq 1\,(1 \leq i \leq k)$ を取り，

$$\log B \geq \max_{1 \leq i \leq k}\{1, h(\beta_i)\}.$$

となる実数 B を考える．もし $\beta_1 u_1 + \cdots + \beta_k u_k \neq 0$ ならば effective な C で k, p にのみよる正定数が存在して次を満たす；

$$\begin{gathered}\log|\beta_1 u_1 + \cdots \beta_k u_k|_v \geq \\ -C \cdot D^{2k+2}\,(\log B + h + \log\log V_1 + \log DU_1) \\ \times (\log\log V_1 + h + \log DU_1)^{k+1} \times \prod_{i=1}^{k}(h + \log V_i + \log U_i)\end{gathered}$$

(これらの log は通常の Archimedean logarithms である)．

周期の無い関数しか考えていないのだから，これは直接「周期予想」に体する寄与は勿論与え得ない．しかし p 進楕円関数の近似としては始めての一般 k 項の一次形式に対する結果である．そして楕円曲線上の S 整数点の計算にはこの近似が必要である．

5　p 進対数一次形式と abc 予想

ここでは abc 予想に体する p 進対数一次形式のディオファントス近似の寄与が，どの程度可能かを述べよう．楕円対数ではなく，通常の指数関数の逆関数としての対数関数，但し p 進のそれを考えることになる．まず abc 予想を述べる．

Conjecture 1 a, b, c を互いに素な正整数で $a + b = c$ を満たすとする．このとき任意の $\varepsilon > 0$ に対して，ε にのみ依るある定数 $C_1(\varepsilon) > 0$ が存在して

$$c \leq C_1(\varepsilon) N^{1+\varepsilon}$$

が成立する．但し $N = \prod_{p|abc} p$.

これに対して p 進対数一次形式の評価から次が得られる．Tijdeman, Stewart, Yu らの寄与があり，次の定理は 2001 年の Stewart-Yu[Ste-T] による．

Theorem 3 a, b, c を互いに素な正整数で $a+b=c$ を満たすとする．このとき任意の $\varepsilon > 0$ に対して，ε にのみ依るある effective な定数 $C_2(\varepsilon) > 0$ が存在して

$$c \leq \exp(C_2(\varepsilon) N^{\frac{1}{3}} (\log N)^3)$$

が成立する（$N = \prod_{p|abc} p$）．

さて，どのようにすればこの定理が p 進対数一次形式から得られるかを見てみよう．上の Stewart-Yu より弱い結果であるが簡単のために

$$c \leq \exp(C_3 N^5 (\log N)^3)$$

を導いてみよう．

$r := \omega(abc)$ すなわち abc の異なる素因数の個数とおく．素数定理よりある定数 $\kappa_1 > 0$ が存在して

$$\left(\frac{r+3}{\kappa_1}\right)^{r+3} \leq \prod_{j=1}^{r} \frac{p_j}{\log p_j}$$

となる．ここで $p_1, p_2, \cdots, p_j, \cdots,$ とは増大する素数列とする．

$$ord_p c = ord_p \frac{c}{-b} = ord_p \left(\frac{a}{-b} - 1\right) \leq ord_p \left((\frac{a}{b})^4 - 1\right)$$

であるから（ここで $\frac{a}{b}$ の 4 乗が来るのは技巧的な理由によるが，不等式は成立するので正しい）に対して，Yu による「p 進対数一次形式の評価」[Yu] という，いわば「代数的数の累乗の積 -1」の形の数に対する ord_p の上からの（下からではない）評価式を用いると定数 $\kappa_2 > 0$ が存在して

$$ord_p c \leq (\kappa_2 r)^r p^2 \log\log c \cdot \log\log N \cdot \prod_{p|ab} \log p$$

である．さて

$$\log c = \sum_{p|c} (ord_p c) \log p \leq \max_{p|c} (ord_p c) \cdot \log N$$

に上の $ord_p c$ の評価と $\left(\frac{r+3}{\kappa_1}\right)^{r+3}$ の評価を代入すると，荒っぽいが

$$\frac{\log c}{\log\log c} \le N^5(\log N)(\log\log N)$$

すなわち

$$c \le \exp(C_3 N^5(\log N)^3)$$

が出る (C_3 はある effective 正定数)．

このように p 進対数一次形式の評価から abc の弱い評価が出るので，p 進対数一次形式の評価が非常に強ければ，abc 予想も解けて不思議は無い．ではどの程度の p 進対数一次形式の評価ならば abc 予想が解決するであろうか，その一つに A. Baker の予想がある．まず modified - abc 予想を述べよう：

Conjecture 2 a, b, c を互いに素な正整数で $a+b=c$ を満たすとする．このとき任意の $\varepsilon>0$ に対して，ε にのみ依るある定数 $C_4(\varepsilon)>0$ と，絶対定数 $\kappa>0$ が存在して

$$c \le C_4(\varepsilon)\cdot\varepsilon^{-\kappa\omega(ab)}N^{1+\varepsilon}$$

が成立する．但し $N=\prod_{p|abc}p$.

これは次の p 進対数一次形式の評価予想から得られる：

Conjecture 3 $b_1,\cdots,b_k$ は全ては零でない整数，$a_1,\cdots,a_k$ は正整数とする．$\Lambda := b_1\log a_1+\cdots+b_k\log a_k$ とおく．また

$$\Xi := \min\{1,|\Lambda|\}\prod_p \min\{1, p|\Lambda|_p\}$$

とおく．この $\prod_p$ は全ての素数を走るとする．このときある（effective な）定数 $C_5>0$ が存在して

$$\log\Xi \le C_5\log\max\{|b_1|,\cdots,|b_k|\}\cdot\left(\sum_{i=1}^{k}\log a_i\right)$$

を満たす．

この p 進対数一次形式の評価予想において何らかの進展を見る事が出来れば，それは abc について現在知られている結果の改良を与えうる．現在 $\log\Xi \le C_5\log\max\{|b_1|,\cdots,|b_k|\}\cdot\left(\sum_{i=1}^{k}\log a_i\right)$ の和のところが積になっている評価迄しか存在していない．そして積の部分を和に改良するのは現在のところ方法がない．

References

[Be] D. BERTRAND, *Série d'Eisenstein et transcendance*, Bull. Soc. Math. France, **104**, 1976, 309–321..

[Da] S. DAVID, *Autour d'une conjecture de S. Lang*, Approximations Diophantiennes et Nombres Transcendants, ed. P. Philippon, Walter de Gruyter, 1992, 65–98.

[Da-Hi1] S. DAVID and N. HIRATA-KOHNO, *Recent progress on linear forms in elliptic logarithms*, in the Proceedings of the Conference *A Panorama in Number Theory*, G. WÜSTHOLZ ed., Cambridge University Press, 2002, 26–37.

[Da-Hi2] S. DAVID and N. HIRATA-KOHNO, *Linear Forms in Eliptic Logarithms*, sibmitted.

[Da-Hi3] S. DAVID and N. HIRATA-KOHNO, *Logarithmic Functions and Formal Groups of Elliptic Curves*, preprint.

[Par-Schf] A. N. PARSHIN and I. R. SCHFAREVICH (eds.), N. I. Fel'dman and Yu. V. NESTERENKO (authors), *Number Theory IV*, Encyclopaedia of Mathematical Sciences vol. **44**, 1998.

[Ro] P. ROQUETTE *Analytic theory of elliptic function*, Hamburger Math. Einzelschriften, Neue Folge, Heft 1, Vandenhoeck & Ruprecht in Göttingrn, 1970.

[Schn] Th. SCHNEIDER, *Einführung in die transzendenten Zahlen*, Springer-Verlag, 1957.

[Ste-T] C. L. STEWART and R. TIJDEMAN, *On the Oesterlé-Masser conjecture*, Monatsh. Math., **102**, 1986, 251–257.

[Ste-Yu1] C. L. STEWART and Kunrui YU, *On the abc conjecture*, Math. Ann., **291**, 1991, 225–230.

[Ste-Yu2] C. L. STEWART and Kunrui YU, *On the abc conjecture II*, Duke Math. J. **108**, 2001, 169–181.

[Wal] M. WALDSCHMIDT, *Nombres transcendants et groupes algébriques*, Astérisque, vol. **69/70**, 1979.

[Yu] Kunrui YU, *Report on p-adic logarithmic forms*, in the Proceedings of the Conference *A Panorama in Number Theory*, G. WÜSTHOLZ ed., Cambridge University Press, 2002, 11–25.

Noriko HIRATA-KOHNO
Dept. of Mathematics
College of Science and Technology
NIHON University
Kanda, Chiyoda, Tokyo 101-8308
JAPAN